



DEPARTMENT OF VETERANS AFFAIRS

Privacy Act of 1974; System of Records

AGENCY: Department of Veterans Affairs (VA), Veterans Health Administration (VHA).

ACTION: Notice of a Modified System of Records.

SUMMARY: As required by the Privacy Act of 1974, notice is hereby given that the Department of Veterans Affairs (VA) is modifying the system of records entitled “Ethics Consultation Web-based Database (ECWeb)-VA” (152VA10P6). VA is modifying the system by revising the System Name; System Number; System Location; Purpose of the System; Categories of Records in the System; Record Source Categories; Routine Uses of Records Maintained in the System; Policies and Practices for Storage of Records; Policies and Practices for Retention and Disposal of Records; and Physical, Procedural, and Administrative Safeguards. VA is republishing the system notice in its entirety.

DATES: Comments on this modified system of records must be received no later than 30 days after date of publication in the Federal Register. If no public comment is received during the period allowed for comment or unless otherwise published in the Federal Register by VA, the modified system of records will become effective a minimum of 30 days after date of publication in the Federal Register. If VA receives public comments, VA shall review the comments to determine whether any changes to the notice are necessary.

ADDRESSES: Comments may be submitted through www.Regulations.gov or mailed to VA Privacy Service, 810 Vermont Avenue, NW, (005R1A), Washington, DC 20420.

Comments should indicate that they are submitted in response to “Ethics Consultation Web-based Database (ECWeb)-VA (152VA10P6)”. Comments received will be available at [regulations.gov](https://www.regulations.gov) for public viewing, inspection or copies.

FOR FURTHER INFORMATION CONTACT: Stephania Griffin, Veterans Health

Administration (VHA) Privacy Officer, Department of Veterans Affairs, 810 Vermont Avenue, NW, Washington, DC 20420; telephone (704) 245-2492 (Note: this is not a toll-free number).

SUPPLEMENTARY INFORMATION: The System Name will be changed from “Ethics Consultation Web-based Database (ECWeb)-VA” to “IntegratedEthics Web Database (IEWeb)-VA”. The System Number will be changed from 152VA10P6 to 152VA10 to reflect the current VHA organizational routing symbol.

The System Location is being updated to remove automated records within ECWeb maintained on a VA server administered by VA, 810 Vermont Avenue NW., Washington, DC. This section will include IntegratedEthics Web Database (IEWeb) may be maintained on Salesforce Development Platform (SFDP) VA and is hosted in a Federal Risk Authorization Management Program (FedRAMP) certified cloud, as administered by Salesforce at 44521 Hastings Dr., Building 90, Ashburn, VA 20147.

The Purpose is being modified to include ethics quality improvement and documenting ethics activities that do not relate to ethics consultation or ethics quality improvement but are important for the ethical culture and environment of VHA.

The Categories of Records in the System is being modified to include: 2. Preventive Ethics (PE) records document work done to address recurring ethical concerns by applying quality improvement methods to identify and address ethics gaps on a systems level including intake forms and project record forms. PE records may include the name and contact information of VA employees as well as information about ethical standards, best ethics practices, current state, ethics quality gap, improvement goals, domains and topics, impact on patients and/or staff, prioritization, results, volume or scope of effect. 3. Ethics Activity Log (EAL) records document education, training, clinical and administrative rounding, referrals and other ethics activities that do not relate

to ethics consultation or preventive ethics activities. EAL records may include the name and contact information of VA employees as well as information such as a description of the ethics activity, domain, topic, time spent.

The Record Source Categories is being modified to include “Patient Medical Records-VA” (24VA10A7), “Veterans Health Information System and Technology Architecture (VistA) Records-VA” (79VA10), and electronic health record systems.

The Routine Uses of Records Maintained in the System will delete routine use #20, which was a duplicate of Routine Use #2. The following Routine Uses will be deleted:

8. Relevant health care information may be disclosed to a non-VA nursing home facility that is considering the patient for admission, when information concerning the individual’s medical care is needed for the purpose of preadmission screening under 42 CFR 483.20(f), for the purpose of identifying patients who are mentally ill or mentally retarded, so they can be evaluated for appropriate placement.

9. Relevant health care information may be disclosed to a State Veterans Home for the purpose of medical treatment and/or follow-up at the State Home when VA makes payment of a per diem rate to the State Home for the patient receiving care at such home, and the patient receives VA medical care.

10. Relevant health care information may be disclosed to (a) A Federal agency or non-VA health care provider or institution when VA refers a patient for hospital or nursing home care or medical services, or authorizes a patient to obtain non-VA medical services and the information is needed by the Federal agency or non-VA institution or provider to perform the services; or (b) a Federal agency or a non-VA hospital (Federal, state and local, public or private) or other medical installation having hospital facilities, blood banks, or similar institutions, medical schools or clinics, or other groups or individuals that have contracted or agreed to provide medical services, or share the use of medical resources under the provisions of 38 U.S.C. 513, 7409, 8111, or 8153, when treatment is rendered

by VA under the terms of such contract or agreement or the issuance of an authorization, and the information is needed for purposes of medical treatment and/or follow-up, determining entitlement to a benefit or, for VA to effect recovery of the costs of the medical care.

The following Routine Uses will be added:

8. VA may disclose information from this system to another Federal agency or Federal entity, when VA determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

9. VA may disclose information to: (1) a Federal agency or health care provider when VA refers a patient for medical and other health services, or authorizes a patient to obtain such services and the information is needed by the Federal agency or health care provider to perform the services; or (2) a Federal agency or to health care provider under the provisions of 38 U.S.C. 513, 7409, 8111, or 8153, when treatment is rendered by VA under the terms of such contract or agreement or the issuance of an authorization, and the information is needed for purposes of medical treatment or follow-up, determination of eligibility for benefits, or recovery by VA of the costs of the treatment.

10. VA may disclose information to the National Practitioner Data Bank at the time of hiring or clinical privileging/re-privileging of health care practitioners, and other times as deemed necessary by VA, in order for VA to obtain information relevant to a Department decision concerning the hiring, privileging/re-privileging, retention, or termination of the applicant or employee.

The following Routine Uses will be modified.

15. VA may disclose information to the DoJ or in a proceeding before a court, adjudicative body, or other administrative body before which VA is authorized to appear, when:

- (a) VA or any component thereof;
- (b) Any VA employee in his or her official capacity;
- (c) Any VA employee in his or her official capacity where DoJ has agreed to represent the employee; or
- (d) The United States, where VA determines that litigation is likely to affect the agency or any of its components,

is a party to such proceedings or has an interest in such proceedings, and VA determines that use of such records is relevant and necessary to the proceedings.

16. VA may disclose information that, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, to a Federal, state, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law. The disclosure of the names and addresses of Veterans and their dependents from VA records under this routine use must also comply with the provisions of 38 U.S.C. 5701.

Policies and Practices for Storage of Records is being modified to remove copies of back up computer files being maintained at an off-site location. This section will include that records are maintained on the VA Salesforce Government Cloud (i.e., Federal Risk Authorization Management Program (FedRAMP) certified cloud).

Policies and Practices for Retention and Disposal of Records is being modified to replace Record Control Schedule (RCS) 10-1 Item # XLIII-2, with RCS 10-1 item 6000.2. Also, General Records Schedule (GRS) 25 Items 1.a and 1.b (N1-GRS-01-1 item 1a & 1b) will be replaced with, GRS 2.8 Item 010.

Physical, Procedural, and Administrative Safeguards (Access) is being modified to remove:

1. Access to VA working and storage areas is restricted to VA employees on a “need-to-know” basis; strict control measures are enforced to ensure that disclosure to these individuals is also based on this same principle. Generally, VA file areas are locked after normal duty hours and the facilities are protected from outside access by the Federal Protective Service or other security personnel.
2. Access to computer rooms at health care facilities is generally limited by appropriate locking devices and restricted to authorized VA employees and vendor personnel. Automated Data Processing (ADP) peripheral devices are placed in secure areas (areas that are locked or have limited access) or are otherwise protected. Information in ECWeb may be accessed by authorized VA employees. Access to file information is controlled at two levels; the systems recognize authorized employees by series of individually unique passwords/codes as a part of each data message, and the employees are limited to only that information in the file, which is needed in the performance of their official duties. Information that is downloaded from ECWeb and maintained on personal computers is afforded similar storage and access protections as the data that is maintained in the original files. Access to information stored on automated storage media at other VA locations is controlled by individually unique passwords/codes.
3. Access to computer rooms is restricted to authorized operational personnel through electronic locking devices. All other persons gaining access to computer rooms are escorted. Information stored in the computer may be accessed by authorized VA employees at remote locations including VA health care facilities, Information Systems Centers, VA Central Office, and Veteran Integrated Service Networks. Access is controlled by individually unique passwords/codes, which must be changed periodically by the employee. This section will now state, Salesforce Government Cloud is maintaining underlying physical infrastructure. Additional Interconnection Security Agreement (ISA) and Memorandum of

Understanding (MOU) are required between the VA and VA designated contractors/vendors that own the data that is stored or processed within Salesforce Development Platform VA. The vendor-specific agreements will describe the data ownership and storage requirements. The parties agree that transmission, storage and management of VA sensitive information residing in the Salesforce Development Platform VA is the sole responsibility of VA employees or designated contractors/vendors assigned to manage the system. At no time will Salesforce Government Cloud have any access to VA data residing within the Salesforce Development Platform VA. Thus, all agreements on data and system responsibilities shall not be covered in this base agreement (i.e., MOU). However, Salesforce Government Cloud shall provide the tools to allow VA to properly secure all systems and data hosted in the Salesforce Development Platform VA.

The Report of Intent to Modify a System of Records Notice and an advance copy of the system notice have been sent to the appropriate Congressional committees and to the Director of the Office of Management and Budget (OMB) as required by 5 U.S.C. 552a(r) (Privacy Act) and guidelines issued by OMB (65 FR 77677), December 12, 2000.

Signing Authority

The Senior Agency Official for Privacy, or designee, approved this document and authorized the undersigned to sign and submit the document to the Office of the Federal Register for publication electronically as an official document of the Department of Veterans Affairs. Neil C. Evans, M.D., Chief Officer, Connected Care, Performing the Delegable Duties of the Assistant Secretary for Information and Technology and Chief Information Officer, approved this document on October 19, 2021 for publication.

Dated: November 24, 2021.

Amy L. Rose,

Program Analyst,

VA Privacy Service,

Office of Information Security,

Office of Information and Technology,

Department of Veterans Affairs.

SYSTEM NAME AND NUMBER: IntegratedEthics Web Database (IEWeb)-VA

(152VA10)

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Automated records within the IntegratedEthics Web Database (IEWeb) may be maintained on Salesforce Development Platform (SFDP) VA and is hosted in a Federal Risk Authorization Management Program (FedRAMP) certified cloud, as administered by Salesforce at 44521 Hastings Dr., Building 90, Ashburn, VA 20147.

SYSTEM MANAGER(S): Official responsible for policies and procedures: Toby Schonfeld, PhD, Executive Director, National Center for Ethics in Health Care, Veterans Health Administration, Department of Veterans Affairs, 810 Vermont Avenue, N.W., Washington, DC 20420. Telephone (202)-461-1750 (Note: this is not a toll-free number).

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, U.S.C., 501(b), 304, 7301, and 7304(a).

PURPOSE(S) OF THE SYSTEM: The records may be used for such purposes as: education about ethics consultation; ongoing treatment of the patient; documentation of treatment provided; payment; healthcare operations such as producing various management and patient follow-up reports; responding to patient and other inquiries; for ethics quality improvement; for documenting ethics activities that do not relate to ethics consultation or ethics quality improvement but are important for the ethical culture and environment of VHA; for epidemiological research and other healthcare related studies; statistical analysis, resource allocation and planning; providing clinical and administrative support to patient healthcare; audits, reviews and investigations conducted by staff of the healthcare facility, the VISN's, VA Central Office, and the VA Office of Inspector General (OIG); sharing of health information between and among VHA, Department of Defense (DoD), Indian Health Services (IHS), and other government and private industry healthcare organizations; quality improvement/ assurance audits, reviews and

investigations; personnel management and evaluation; employee ratings and performance evaluations, and employee disciplinary or other adverse action, including removal; advising healthcare professional licensing or monitoring bodies or similar entities of activities of VA and former VA healthcare personnel; and, accreditation of a VA healthcare facility by an entity such as The Joint Commission (TJC).

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: The records include information concerning.

1. Veterans who have applied for healthcare services under Title 38, U.S.C., Chapter 17, and members of their immediate families.
2. Spouse, surviving spouse, and children of Veterans who have applied for healthcare services under Title 38, U.S.C., Chapter 17.
3. Other requesters or participants from outside VA for whom personal information will be collected.
4. Individuals examined or treated under contract or resource sharing agreements.
5. Individuals examined or treated for research or donor purposes.
6. Individuals who have applied for Title 38 benefits, but who do not meet the requirements under Title 38 to receive such benefits.
7. Individuals who were provided medical care under emergency conditions for humanitarian reasons.
8. Pensioned members of allied forces provided healthcare services under Title 38, U.S.C., Chapter I.
9. Current and former employees.
10. Contractors employed by VA.

CATEGORIES OF RECORDS IN THE SYSTEM: There are three types of records in IEWeb:

1. Ethics Consultation (EC) records document the consultation request, relevant

consultation specific information, a summary of the information including the ethical analysis and moral deliberation, the explanation of the findings to relevant parties, and support of the consultation process. EC records also include related notes and attachments.

These records may include information related to ethics consultations performed in and for VHA healthcare facilities. Information may include relevant information from a health record (e.g., a cumulative account of sociological, diagnostic, counseling, rehabilitation, drug and alcohol, dietetic, medical, surgical, dental, psychological, and/or psychiatric information compiled by VA professional staff and non-VA healthcare providers); subsidiary record information (e.g., tumor registry, dental, pharmacy, nuclear medicine, clinical laboratory, radiology, and patient scheduling information); identifying information (e.g., name, address, date of birth, partial Social Security number), military service information (e.g., dates, branch and character of service, service number, health information), family or authorized surrogate information (e.g., next-of-kin and person to notify in an emergency), employment information (e.g., occupation, employer name and address), and information pertaining to the individual's medical, surgical, psychiatric, dental, and/or treatment (e.g., information related to the chief complaint and history of present illness; information related to physical, diagnostic, therapeutic, special examinations, clinical laboratory, pathology and x-ray findings, operations, medical history, medications prescribed and dispensed, treatment plan and progress, consultations; photographs taken for identification and medical treatment, education and research purposes; facility locations where treatment is provided; observations and clinical impressions of healthcare providers to include identity of providers and to include, as appropriate, the present state of the patient's health, an assessment of the patient's emotional, behavioral, and social status, as well as an assessment of the patient's rehabilitation potential and nursing care needs). In addition, EC records may include the

name(s) and contact information of healthcare providers, and information regarding healthcare rendered by those providers.

2. Preventive Ethics (PE) records document work done to address recurring ethical concerns by applying quality improvement methods to identify and address ethics gaps on a systems level including intake forms and project record forms. PE records may include the name and contact information of VA employees as well as information about ethical standards, best ethics practices, current state, ethics quality gap, improvement goals, domains and topics, impact on patients and/or staff, prioritization, results, volume or scope of effect.

3. Ethics Activity Log (EAL) records document education, training, clinical and administrative rounding, referrals and other ethics activities that do not relate to ethics consultation or preventive ethics activities. EAL records may include the name and contact information of VA employees as well as information such as a description of the ethics activity, domain, topic, and time spent.

RECORD SOURCE CATEGORIES: Information in this system of records is provided by the patient, family members or accredited representative, and friends, authorized surrogates, healthcare agents, employees, contractors, medical service providers, and various automated systems providing clinical and managerial support at VA healthcare facilities, “Patient Medical Records-VA” (24VA10A7), “Veterans Health Information System and Technology Architecture (VistA) Records-VA” (79VA10), and VA electronic health record systems.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING

CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES: To the extent that records contained in the system may include information protected by 45 CFR parts 160 and 164, *i.e.*, individually identifiable health information, and 38 U.S.C. 7332, *i.e.*, medical treatment information related to drug abuse, alcoholism or alcohol abuse,

sickle cell anemia, or infection with the Human Immunodeficiency Virus, that information may not be disclosed under a routine use unless there is also specific statutory authority in 38 U.S.C. 7332 and regulatory authority in 45 CFR parts 160 and 164 permitting disclosure.

1. VA may disclose information to Federal, state, and local government agencies and national health organizations as reasonably necessary to assist in the development of programs that will be beneficial to claimants, to protect their rights under law, and assure that they are receiving all benefits to which they are entitled.
2. Information may be disclosed by appropriate VA personnel to the extent necessary, on a need-to-know basis, and consistent with good medical-ethical practices, to family members or the persons with whom the patient has a meaningful relationship.
3. VA may disclose information relevant to a claim of a Veteran or beneficiary, such as the name, address, the basis and nature of a claim, amount of benefit payment information, medical information, and military service and active duty separation information, only at the request of the claimant to accredited service organizations, VA-approved claim agents, and attorneys acting under a declaration of representation, so that these individuals can aid claimants in the preparation, presentation, and prosecution of claims under the laws administered by VA.
4. VA may disclose information to attorneys, insurance companies, employers, third parties liable or potentially liable under health plan contracts, and courts, boards, or commissions as relevant and necessary to aid VA in the preparation, presentation, and prosecution of claims authorized by law.
5. VA may disclose information from this system to epidemiological and other research facilities approved by the Under Secretary for Health for research purposes determined to be necessary and proper, provided that the names and addresses of Veterans and their dependents will not be disclosed unless those names and addresses are first

provided to VA by the facilities making the request.

6. VA may disclose information to another Federal agency, court, or party in litigation before a court or in an administrative proceeding conducted by a Federal agency, when the government is a party to the judicial or administrative proceeding.
7. Information concerning a non-judicially declared incompetent patient may be disclosed to a third party upon the written request of the patient's next-of-kin in order for the patient, or, consistent with the best interest of the patient, a member of the patient's family, to receive a benefit to which the patient or family member is entitled or to arrange for the patient's discharge from a VA medical facility. Sufficient data to make an informed determination will be made available to such next-of-kin. If the patient's next-of-kin is not reasonably accessible, the Chief of Staff, Director, or designee of the custodial VA medical facility may disclose the information for these purposes.
8. VA may disclose information from this system to another Federal agency or Federal entity, when VA determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.
9. VA may disclose information to: (1) a Federal agency or health care provider when VA refers a patient for medical and other health services, or authorizes a patient to obtain such services and the information is needed by the Federal agency or health care provider to perform the services; or (2) a Federal agency or to health care provider under the provisions of 38 U.S.C. 513, 7409, 8111, or 8153, when treatment is rendered by VA under the terms of such contract or agreement or the issuance of an authorization, and the information is needed for purposes of medical treatment or follow-

up, determination of eligibility for benefits, or recovery by VA of the costs of the treatment.

10. VA may disclose information to the National Practitioner Data Bank at the time of hiring or clinical privileging/re-privileging of health care practitioners, and other times as deemed necessary by VA, in order for VA to obtain information relevant to a Department decision concerning the hiring, privileging/re-privileging, retention, or termination of the applicant or employee.
11. Information from an IEWeb record which relates to the performance of a healthcare student or provider may be disclosed to a medical or nursing school, or other healthcare related training institution, or other facility with which there is an affiliation, sharing agreement, contract, or similar arrangement when the student or provider is enrolled at or employed by the school or training institution, or other facility, and the information is needed for personnel management, rating and/or evaluation purposes.
12. VA may disclose information from this system of records to individuals, organizations, private or public agencies, or other entities or individuals with whom VA has a contract or agreement to perform such services as VA may deem practicable for the purposes of laws administered by VA, in order for the contractor, subcontractor, public or private agency, or other entity or individual with whom VA has a contract or agreement to perform services under the contract or agreement. This routine use includes disclosures by an individual or entity performing services for VA to any secondary entity or individual to perform an activity that is necessary for individuals, organizations, private or public agencies, or other entities or individuals with whom VA has a contract or agreement to provide the service to VA.
13. VA may disclose information to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

14. VA may disclose information to National Archives and Records Administration (NARA) in records management inspections conducted under 44 U.S.C. 2904 and 2906, or other functions authorized by laws and policies governing NARA operations and VA records management responsibilities.

15. VA may disclose information to the DoJ or in a proceeding before a court, adjudicative body, or other administrative body before which VA is authorized to appear, when:

- (a) VA or any component thereof;
- (b) Any VA employee in his or her official capacity;
- (c) Any VA employee in his or her official capacity where DoJ has agreed to represent the employee; or
- (d) The United States, where VA determines that litigation is likely to affect the agency or any of its components,

is a party to such proceedings or has an interest in such proceedings, and VA determines that use of such records is relevant and necessary to the proceedings.

16. VA may disclose information that, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, to a Federal, state, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law. The disclosure of the names and addresses of Veterans and their dependents from VA records under this routine use must also comply with the provisions of 38 U.S.C. 5701.

17. VA may disclose information to other Federal agencies to assist such agencies in preventing and detecting possible fraud or abuse by individuals in their operations and programs.

18. VA may disclose any information or records to appropriate agencies, entities, and persons when (1) VA suspects or has confirmed that there has been a breach of the

system of records; (2) VA has determined that as a result of the suspected or confirmed breach there is a risk to individuals, VA (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, or persons reasonably necessary to assist in connection with VA efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

19. VA may disclose information to survey teams of The Joint Commission, College of American Pathologists, American Association of Blood Banks, and similar national accreditation agencies or boards with which VA has a contract or agreement to conduct such reviews, as relevant and necessary for the purpose of program review or the seeking of accreditation or certification.

20. VA may disclose ethics consultation records to groups (e.g., American Society for Bioethics and the Humanities) performing improvement or quality assessments as part of approved research or quality improvement projects with respect to ethics consultation practices.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are maintained on the VA Salesforce Government Cloud (i.e., Federal Risk Authorization Management Program (FedRAMP) certified cloud). Subsidiary record information is maintained at the various respective IntegratedEthics services within the VHA healthcare facility and by individuals, organizations, and/or agencies with whom VA has a contract or agreement to perform such services, as the VA may deem practicable.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records are retrieved by record number, name of ethics consultant and other VA staff, requester, ethics domain or topic, facility, keywords or phrases.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:
Records that are stored within Computerized Patient Record System (CPRS) and

Veterans Health Information Systems and Technology Architecture (VistA) will be maintained in accordance with Record Control Schedule (RCS) 10-1 Item 6000.2, Electronic Health Records, NARA job# N1-15-02-3. All other records maintained outside the Electronic Health Record will be maintained in accordance with General Records Schedule (GRS) 2.8 Ethics Program Records Item 010.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Salesforce Government Cloud is maintaining underlying physical infrastructure. Additional ISA and MOU are required between the VA and VA designated contractors/vendors that own the data that is stored or processed within Salesforce Development Platform VA. The vendor-specific agreements will describe the data ownership and storage requirements. The parties agree that transmission, storage and management of VA sensitive information residing in the Salesforce Development Platform VA is the sole responsibility of VA employees or designated contractors/vendors assigned to manage the system. At no time will Salesforce Government Cloud have any access to VA data residing within the Salesforce Development Platform VA. Thus, all agreements on data and system responsibilities shall not be covered in this base agreement (i.e., MOU). However, Salesforce Government Cloud shall provide the tools to allow VA to properly secure all systems and data hosted in the Salesforce Development Platform VA.

RECORD ACCESS PROCEDURE: Individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA healthcare facility location where they are or were employed or made contact or they may write to the National Center for Ethics in Health Care at 810 Vermont Avenue, NW, Washington, DC 20420.

CONTESTING RECORD PROCEDURES: (See Record Access Procedures above.)

NOTIFICATION PROCEDURE: Individuals seeking information regarding access to and

contesting of IEWeb records may write, call, or visit the last VA healthcare facility where healthcare was provided or by writing to the National Center for Ethics in Health Care at 810 Vermont Avenue, NW, Washington, DC 20420.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: Last full publication provided in 81 FR 5033 dated January 29, 2016.

[FR Doc. 2021-26026 Filed: 11/29/2021 8:45 am; Publication Date: 11/30/2021]